COPYRIGHT NOTICE

[0001] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or patent disclosure as it appears in the Patent and Trademark Office, patent file or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates generally to videoconferencing and video communications and applications based on the technology thereof. More specifically, it relates to a method of creating authoritative documents that verify either an identity, or a signature or the contents of a document during a real-time, live-stream videoconference exchange.

[0004] 2. Description of the Prior Art

[0005] It can be appreciated that methods of videoconferencing have been in

use for years. Typically, there exits a range of videoconference systems or video communication systems that utilize a variety of structures, such as telephone, personal computers and mounted cameras to relay live stream video, and a variety of methods to facilitate the live stream conference. The prior art discloses U.S. Pat. Nos. 6, 317,777 issued to Skarbo et al; 5,712,914 issued to Aucsmith et al; 5,991,276 issued to Yamamoto; 6,124,882 issued to Voois et al; 6,121,998 issued to Voois et al; 6,128,033 issued to Friedel et al; 6,037,970 issued to Kondo and US Patent Application Publication 2001/0002485, filed by Bisbee et al.

[0006] The Skarbo patent discloses a document-collaboration videoconferencing system between a first and a second conference attendee. In one embodiment, the system comprises a document server, a local presenter computing system, and a conferencing computing system. In this embodiment, the local presenter computing system transfers a document to the document server over a network, and the first conferencing system copies such document over the network from the document server. The Skarbo patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[007] The Aucsmith patent discloses method and apparatus of communicating information comprising providing a datum which includes a digital certificate containing data. The digital certificate including an extension which includes: a first identifier which specifies a major classification of the data; a second identifier which specifies a minor classification of the data; and data in a format according to the major classification and the minor classification, the data indicating an owner of the datum and a use for which the datum is intended. The certificate allows authentication of the certificate itself and the data contained therein, and the data contained in the certificate can include information allowing verification of the identity of the holder of the certificate. The Aucsmith patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0008] The Yamamoto patent discloses a multipoint videoconference system which delivers video and voice information along with various types of material data to realize a more realistic teleconferencing environment. The system comprises a plurality of videoconference terminals, a videoconference server, and a videoconference administration server. The videoconference administration server controls network connections between the

videoconference server and the videoconference terminals. The Yamamoto patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0009] The Vois U.S. Pat. No. 6,124,882 discloses a videophone device that utilizes a programmable processor circuit capable of communicating over a conventional communications channel, such as a POTS line, and of generating video data for display on a television set. The device includes a video source, an interface circuit, including a modem transmitting and receiving video and audio data over the channel; a circuit for storing a program to control the videophone apparatus; and a display driver circuit for generating video data to the display. The Vois U.S. Pat. No. 6,124,882 does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0010] The Vois U.S. Pat. No. 6,121,998 discloses a programmable video/general-purpose processor capable of readily updating program-related data. The processor includes a first circuit section used to process data for videoconferencing and to detect codes data used for revising software-relate data provided from a remote location, and a second circuit

section used for executing the executable program data stored in the second memory circuit. A volatile memory circuit is coupled to and accessed by the programmable video/general-purpose processor, and is used for storing the revision data until it is validated. The non-volatile memory circuit is then used by the processor in a subsequent video-related application, such as a videoconferencing application or a web browser application. The Vois patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0011] The Friedel patent discloses an audiovisual communications terminal apparatus that is adapted for interconnection to at least one other audiovisual communications terminal apparatus by a communications medium to form an audiovisual teleconferencing network. The audiovisual communications terminal apparatus includes an interface device, producing and transmitting means, and receiving and broadcasting means. The interface device operates to condition input audiovisual signals received from the other audiovisual communications terminal apparatus and to condition output audiovisual signals for processing by the other audiovisual communication terminal apparatus. The receiving an broadcasting means receive the input audiovisual signals from the interface device and broadcast the received input audiovisual signals thereby

creating an audiovisual teleconference between two users so that the users can both see and hear each other. The Friedel patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0012] The Kondo patent discloses a videoconference system that conducts a videoconference among a plurality of communication centers which are connected by a communication line. Each communication center includes: display devices for displaying images from the other communication centers participating in the videoconference; speaker devices for outputting voices from the other communication centers participating in the videoconference; camera devices disposed at positions corresponding to the display devices, for imaging participants in the videoconference; microphone devices disposed at positions corresponding to the display devices, for capturing voices from the participants; and a transmitter/receiver transmitting output signals from the camera devices and output signals from the microphone devices to the other communication centers, and receiving output signals from the camera devices and output signals from the microphone devices of the other communication centers, the transmitter/receiver for supplying the output signals from the camera devices and

the output signals from the microphone devices of the other communication centers to the display devices and the speaker devices corresponding to the camera devices and the microphone devices. The Kondo patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0013] The Bisbee Publication (pending application) discloses a method of handling stored electronic original objects that have been created by signing information objects by respective transfer agents, submitting signed information objects to a trusted custodial utility, validating the submitted signed information objects by at least testing the integrity of the contents of each signed information object and the validity of the signature of the respective transfer agent, and applying to each validated information object a date-time stamp and a digital signature and authentication certificate of the trusted custodial utility. The Bisbee patent does not disclose a method of creating authoritative documents that verify either an identity, a signature, or the contents of a document via a real-time, live-stream videoconference exchange.

[0014] The prior art and prevailing business practices clearly illustrate the usefulness and many benefits of using videoconference methods and

applications thereof as a means to unite geographically remote parties and to exchange data among the parties. While the prior art discloses very useful means and benefits, the prior art does not disclose a method whereby during the videoconference an authoritative document is created that verifies either an identity, or a signature, or the contents of a document, or a combination thereof.

[0015] The main problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process, whereby an identity, or a signature, or the contents of a document is verified during the videoconference.

[0016] Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby biometric data is input during the videoconference to verify an identity, or a signature, or the contents of a document.

[0017] Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a signature may be notarized by a notary public during the videoconference.

[0018] Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a client may tender a service request for videoconference verification from a remote location using the Internet.

[0019] Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby an authoritative document is created and issued during the videoconference.

[0020] An object of the present invention is to provide a method of real-time, live-stream videoconference, whereby an identity, or a signature, or the contents of a document is verified during the videoconference.

[0021] An object of the present invention is to provide a method of real-time, live-stream videoconference, whereby an authoritative document is created and issued during the videoconference.

[0022] An object of the present invention is to provide a method of real-time, live-stream videoconference whereby a client may request that a notary public notarize an electronic document during the videoconference.

[0023] An object of the present invention is to provide a method of real-time, live-stream videoconference, whereby authoritative documents enable electronic commerce transactions; particularly transactions that involve sensitive data or high value transactions.

[0024] In these respects, the method of identity, or signature, or document authentication via a real-time, live-stream videoconference substantially departs from the conventional concepts and designs of the prior art and provides a method primarily developed for the purpose of verifying an identity, or a signature, or a document via a real-time, live-stream videoconference

SUMMARY OF THE INVENTION

[0025] The general purpose of the present invention, which will be described subsequently in greater detail, is to provide a new method of real- time, live-stream videoconference wherein a client may request verification of an identity (identity being an individual), a signature (signature belonging to an individual), or the contents of a document (document being either hard-copy or electronic), and whereby an authoritative document is created (the authoritative document ("A.D.") is either a hard copy document or electronic record or both).

[0026] The method of the present invention incorporates applications and technology that in conjunction are used to authenticate an individual's identity, or a signature, or a document, during a real-time, live-stream videoconference. The purpose of the present invention is to create and issue an authoritative document ("A.D.") using data input during the videoconference.

[0027] Briefly, the method of the present invention discloses a client requesting authentication services of either an identity, or a signature, or a document from an independent third party provider herein referred to as the " Video Verification Service Center ("VVSC"). In the preferred embodiment of the present invention, the client is governmental agency, such as the DMV, the United States Passport Office, an administrative agency (social security, medi-care, etc), or the United States Postal Service.

[0028] Governmental agencies are dependent on verifying the identity of whom they provide services to, whether it be a driver's license, passport, or healthcare benefits. Likewise, governmental agencies are dependent on verifying the identity of those they employ for security purposes. Said governmental agencies traditionally are ill-equipped to create and issue identification documents, thereby necessitating a need to contract such work to a third party, or to deal with a back-log of service requests, creating greater inefficiency and delays in time. Said

governmental agencies traditionally are ill-equipped to create and issue identification documents, thereby necessitating a need to contract such work to a third party, or to deal with a back-log of service requests, creating greater inefficiency and delays in time. [0028] In the preferred embodiment of the present invention, the client tenders a request for identity verification of an individual. The client could be either a public entity (governmental agency (G.A.)) or a private entity (private party (P.P.)). In the case of the former, the client (GA) would request that an individual visit a VVSC for the purpose of authenticating said individual's identity (for the purpose of clarity, the requesting party, i.e. placing the service request with the VVSC is referred to as "Client", and the individual whose identity is verified is referred to as the "Customer").

[0029] The customer would be required to provide identifying criteria, at least one of a group of an official government identification document (identity document), or a fingerprint, or a signature, or a photograph, or a retinal scan, or a voice print or electronic data such as a password or a code (collectively referred to as the "Identity Criteria").

[0030] The identify criteria are determined by the requesting party, the client. The VVSC verifies the authenticity of the identify criteria provided by the customer. The VVSC establishes a real-time, live-stream videoconference with

the client, whereby the client may witness the verification of the customer. The client may also participate in the videoconference by providing identity criteria, if necessary.

[0031] Upon verifying the identity of the customer, according to the identity criteria established by the client, the VVSC creates an authoritative document (A.D.) that contains the identify criteria. In the preferred embodiment, the authoritative document typically will take the form of an identity card that contains identity criteria provided the customer such as an identity document (drivers license or a passport), signature, fingerprint, and a photograph. Typically, a copy of the authoritative document is sent to the client for archive and the original AD is issued to the customer. Alternatively, the client may request that the identity card (AD) be issued to a designated third party other than the individual. The A.D may also comprise an electronic document, or an electronic record, that is stored in a hard copy device such as a disc or chip.

[0032] With respect to aforementioned process, the method of the present invention is further capable of creating identity cards (authoritative documents) for the private sector (private party), such as airlines and banks using the method disclosed above.

[0033] In another embodiment of the present invention, the client (public or private; G.A. or P.P.) requests verification of an individual's signature, the signature verification may include notarization for transactions required to have the force of law (e.g. the transfer of real property), or where the client chooses to have a notary public witness and authenticate the transaction. Per the method of the preferred embodiment, the client tenders a request to the VVSC for signature verification, and notarization, if required. The identify criteria are determined by the requesting party, the client. The VVSC verifies the authenticity of the identify criteria provided by the customer. The VVSC establishes a real-time, live-stream videoconference with the client, whereby the client may witness the authentication process of the customer's signature and notarization of said signature, and where the client may participate in the videoconference if necessary.

[0034] The electronic document signed by the customer or the client (if required) may be either downloaded from an electronic document repository maintained by the VVSC, or provided by the client and uploaded to the VVSC host computer system.

[0035] Upon verifying the signature of the customer, according to the identity criteria established by the client, the VVSC creates the authoritative document

(A.D.). The A.D. contains the identify criteria along with the signed, notarized, document. Typically, the authoritative document is sent to the client are copies are issued third parties as identified by the client.

[0036] In another embodiment, the client and the customer facilitate an authentication transaction by accessing a website maintained by the inventive device (VVSC website). The client tenders a request for services using the website accessible via the Internet. The request for services may comprise any of the videoconference verification processes disclosed above: identity, or signature, or document authentication.

[0037] As a priori to use verification services via the website, the client and customer must be registered with the VVSC. Registration entails providing the VVSC with identity criteria, as determined by the client/customer (each of whom elects which of the group of identity criteria to register with the VVSC. The identity criteria is retained on file with the VVSC in the form of a registration account for future verification requests by the client which are processed through the website (as opposed to an independent VVSC).

[0038] In the method of a website verification request, the VVSC verifies the authenticity of the identifying criteria provided by the customer for the client during the videoconference, by matching the identity criteria input with the registration account.

[0039] Upon completion of the website service request, the VVSC creates an authoritative document that contains the identifying criteria requested to fulfill the service request. Typically, the authoritative document is issued to the client. Alternatively, the client may request that the authoritative document be issued to a designated third party, either the customer, or another party, such as a bank, lawyer, or other interested party to the transaction.

[0040] There has thus been outlined, rather broadly, the more important features and objectives of the invention in order that the detailed description thereof may be better understood, and in order that the present contribution to the art may be better appreciated. There are additional features of the invention that will be described hereinafter.

[0041] Other objects and advantages of the present invention will become obvious to the reader and it is intended that these objects and advantages are within the scope of the present invention. In this respect, before explaining at

least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of the description and should not be regarded as limiting.

[0042] To the accomplishment of the above and related objects, this invention may be embodied in the form illustrated in the accompanying drawings, attention being called to the fact, however, that the drawings are illustrative only, and that changes may be made in the specific construction illustrated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0043] Various other objects, features and attendant advantages of the present invention will become fully appreciated as the same becomes better understood when considered in conjunction with the accompanying drawings, in which like reference characters designate the same or similar parts throughout the several views, and wherein:

[0044] FIG. 1 discloses a method for identity verification. The distinction between the "public" and "private" domain is whether the service request involves a government/regulatory entity (Governmental Agency/ G.A.) or a private party (Private). The former designation being deemed a "public" process whereby the signature or identity authentication is for the purpose of creating a government or a regulatory based identity document. The latter designation being deemed a "private" process whereby identity authentication is for the purpose of a commercial transaction.

[0045] FIG. 1A discloses the method of identity criteria input by a customer.

[0046] FIG. 2 discloses the method of a public client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC downloads a document from the VVSC electronic document repository.

[0047] FIG. 2A discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC downloads a document from the VVSC electronic document repository.

[0048] FIG. 2B discloses the method of a public client service request for signature verification utilizing a notary public, if necessary and whereby the VVSC uploads a document into the VVSC electronic document repository to enable the service request.

[0049] FIG. 2C discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC uploads a document into the VVSC electronic document repository to enable the service request.

[0050] FIG. 3 discloses the method of a private client service request for identity, or signature, or document verification utilizing the VVSC website.

[0051] FIG. 3A discloses the method of a public client service request for identity, or signature, or document verification utilizing the VVSC website.

[0052] FIG. 3B discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, via the VVSC website, and whereby the client downloads a document from the VVSC electronic document repository to enable the service request.

[0053] FIG. 3C discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, via the VVSC website, and whereby the client uploads a document into the VVSC electronic document repository to enable the service request.

[0054] FIG. 3D discloses the method of a private client registration request to use the services offered via the VVSC website, and whereby the client inputs the identity criteria to establish the client registration account.

[0055] FIG. 3E discloses the method of a public client registration request to use the services offered via the VVSC website, and whereby the client inputs the identity criteria to establish the client registration account.

[0056] The drawings are intended to provide an over-view of the processes of the present invention. There exist various technological applications by which the objectives of the present invention can be realized. The various means or methods by which authentication shall be established are specifically set forth in the embodiment of the invention as put forth below.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0057] The advent of conducting business through an increasingly borderless e-commerce world has resulted in new and novel ways for geographically remote parties to communicate and conduct business. As the foregoing summary clearly illustrates, the present invention has the potential to facilitate transactions where the parties are in different cities, states or even countries. For example, an American traveler who loses a passport in India may find a VVSC in India and have the US passport office create and issue a new passport from Des Moines, Iowa, without the wait, expense or inconvenience of traditional channels. The present invention seeks to unite geographically remote parties via a videoconference to enable the parties to conduct a variety of business transactions that once required physical proximity of the parties; said transactions are disclosed below and depicted in the drawings.

[0058] The method of the present invention functions to make possible three primary client service requests using a videoconference:

(i) To verify the identity of an individual and provide documentation thereof in the form of an authoritative document; or

(ii) To verify the signature of an individual and provide documentation thereof in the form of an authoritative document; or

(iii) To verify the contents of a document and provide documentation thereof in the form of an authoritative document.

[0059] DEFINITIONS

[0065] Given the possible breadth of the present invention's potential, it is to be understood that the following terms as used anywhere in the application herein shall be construed to have the following meanings and functions:

[0060] Video Verification Service Center (VVSC)

[0061] The VVSC is a physical structure, a place of business, where either a client or a customer can go to process a service request, The VVSC is staffed by VVSC employees and is equipped with the infrastructure to enable the service requests, as disclosed herein. The VVSC enables the service request tendered by the client and coordinates the schedule of the parties to the videoconference.

[0062] The VVSC establishes the time and date and locations for the real-time, live-stream videoconference between the client and customer(s). All parties to the videoconference receive a confirmation prior to the videoconference via electronic mail or other forms of messaging, such as text, or mail or telephone, informing said parties of the time, date and location of the videoconference. The parties are advised of the contents of the service request, and the necessary identity criteria that must be provided during the videoconference. The VVSC enables and manages the services requested by the client; irrespective of the different location of the client and customer. The VVSC provides the necessary infrastructure and applications for the videoconference, the service request, and to create the finalized authoritative document.

[0063] Video Verification Service Center Website (VVSC website)

[0064] In the preferred embodiment, the VVSC website is accessible via the Internet. The VVSC website provides the service requests disclosed herein: identity, or signature, or document verification. The VVSC website enables a client or a customer to access authentication services from a local computer system (e.g. their home or office), without having to physically visit a VVSC.

[0065] The VVSC website establishes the time and date and locations for the real-time, live-stream videoconference between the client and customer(s). All

parties to the videoconference receive a confirmation prior to the videoconference via electronic mail or other forms of messaging, such as text, or mail or telephone, informing said parties of the time, date and location of the videoconference. The parties are advised of the contents of the service request, and the necessary identity criteria that must be provided during the website videoconference. The VVSC enables and manages the services requested by the client; irrespective of the different location of the client and customer. The VVSC provides the necessary infrastructure and applications for the website videoconference, the service request, and to create the finalized authoritative document.

[0066] Service Request or Request for Services

[0067] A service request, or request for services; used interchangeably, mean a request from a client for any of the foregoing services from the VVSC or the VVSC website. Specifically: identity verification, or signature verification, or document verification, or any combination thereof. Irrespective of the client's service request, it is processed in the context of a real-time, live-stream videoconference. A client may tender a single service request, or multiple service requests, to be fulfilled in the course of the videoconference.

[0068] Client and Customer

[0069] A client is the individual tendering the service request to the VVSC or the VVSC website. A customer is the individual whose identity, or signature, or documents are being verified. In some transactions, a client may also request that the client's identity, or client's signature, or client's document be authenticated during the videoconference, along with the customer's. By way of example, a client and a customer may wish to verify the identity and signature of one another to conclude a commercial transaction, such as the purchase of real estate, during the videoconference. In this instance, each party would input identifying criteria to be authenticated by the VVSC. It is to be understood that there may be multiple clients, or customers involved in a single videoconference. Collectively, the group of individuals participating in the videoconference are referred to as "the Parties".

[0070] Governmental Agency (Public) and Private Party (Private)

[0071] A distinction is made between the type of client tendering a service request. A public client is deemed to be a governmental agency (G.A.) such as the D.M.V. or the USPS, and a private party is deemed to be an individual or business from the private sector.

[0072] Identifying Criteria or I.D. Criteria

[0073] Identifying criteria, or I.D. criteria; used interchangeably, comprise the data input that was used to authenticate either an identity, a signature, or a document. Likewise, identifying criteria is used to create the authoritative document. The identifying criteria for an individual is at least one of a group of: a signature, a fingerprint, a retina scan, a voiceprint, a hard copy identity document, a photograph, or a password/ code. The identifying criteria for a corporate entity is at least one of a group of Depending on the service request, a client may select any combination of the I.D. criteria to authenticate the customer, and any combination of the I.D. criteria to create the authoritative document. The identifying criteria of a public entity include at least one of a group of a hard-copy identity document 46, a password/ code 49, a signature 50, proof of executive identity/authority, a corporation number 232, or a photograph 52.

[0074] Verification or Authentication

[0075] Verification, or authentication (and variations on the verb thereof), are used interchangeably, and mean the process whereby either an identity, or a signature, or a document is verified (or authenticated) in accordance with the client's service request.

[0076] Authoritative Document (A.D.)

[0077] The authoritative document contains the identity criteria information requested by the client in the service request. Depending on the service request, the resulting authoritative document is comprised of at least one of the following group: a signature, a fingerprint, a retina scan, a voiceprint, a hard copy identity document, a photograph, or a password/ code. The authoritative document is created during the real-time, live-stream videoconference. The authoritative document is issued during the real-time, live-stream videoconference. In the preferred embodiment, the authoritative document is issued in the form of an identity card such as a passport or drivers license. The authoritative document can also be issued as an electronic document or electronic code that is stored in a hardware device, such as a disc or chip. Regardless of the form of the authoritative document, each authoritative document is encrypted with the I.D. criteria input and secured with a time and date stamp.

[0078] Videoconference or Webconference

[0079] The term videoconference or webconference means a real-time, live-stream video-communication between the parties . The present invention may use various videoconference technologies and applications thereof, but all are premised on the fact that it is a real time, live stream transaction between the parties that are remote in location. The videoconference enables the exchange of

visual and audio communication between the parties, in addition to enabling the transaction of the service request.

[0080] Document

[0081] An electronic document is used in the method of the present invention. The function of the electronic document repository is to fulfill the client service request. The electronic document may comprise audio, video, graphic, biometric, or text data. A client may elect to download an electronic document from an electronic document repository maintained by the present invention. Alternatively, a client may elect to upload an electronic document to enable the client service request. The VVSC electronic document repository contains a library of electronic documents typically used in public and private party transactions: Oaths, promissory notes, deeds, etc.. It is to be understood, that reference to a document means an electronic document, except where qualified as a hard copy document.

[0082] Electronic Signature Capture Device

[0083] An electronic signature capture device is used in the method of the present invention. The electronic signature capture device captures the electronic signatures of the parties to the transaction. The electronic signature capture device is capable of assigning digital code, or a graphic image, or both to the

authoritative document. The graphical representation depicts the actual hand-written signature of the signatory.

[0084] Signature

The term signature shall be construed to mean any form of electronic signature, including at least one of the group of a graphical, hand written representation, a digital certificate, a password, or other electronic data input qualified to constitute a signature.

[0085] Notary Public and Notarization

[0086] The term notary public and notarization means the process of authenticating a electronic document by a live, human-being commissioned notary public. The notary public notarizes the document in accordance with the law.

[0087] Electronic Notary Device

[0088] An electronic notary device is used for the method of the present invention. The electronic notary device provides a method of electronic notarization to verify a signature or an individual or the contents of a document. An electronic notary stamp is affixed to a document in one of two ways: by manually imprinting the notary seal using the electronic signature capture device

pad, or, alternatively, by utilizing an electronic device that is encrypted with the equivalent of the notary's stamp in the form of source code which embeds the notary code in the authoritative document.

APPLICATIONS OF THE PRESENT INVENTION

[0089] 1. Identity Authentication Using a VVSC (Figs 1-1A)

[0090] 2. Signature Authentication Using a VVSC (Figs2-2C)

[0091] 3. Identity or Signature Authentication Using a VVSC Website (Figs 3-3E)

[0092] Turning now-to the drawings, in which similar reference characters denote similar elements throughout the several views, the attached figures illustrate a method of identity and signature and document authentication, the process of which is comprised of the following steps:

[0093] Figures 1-1A Request for Services from VVSC (Identify Verification)

[0094] In the preferred embodiment, the public client (GA) 15 tenders a service request 10 for identity verification services to the VVSC. The service request 10 entails the client 15 selecting the ID criteria 20 to be used to create the

authoritative document 70. The service request 10 further includes information necessary for the VVSC to accept the service request 10 (total services requested, client's 15 contact information, customer's contact information). The service request 10 also contains information regarding to whom the authoritative document 70 is to be issued to: either the client, the customer, or a third party designated by the client. In the preferred embodiment, the service request 10 specifies that the authoritative document 70 be issued as a hard-copy identity document.

[0095] Upon receipt of the service request 10, the VVSC accepts client service request 25. Acceptance entails a VVSC employee registering the service request 10 in a database to manage the service request 10 during the videoconference 40. Registration of information in the service request 10 is for the sole purpose of enabling the request for services 10. Upon completion of the service request 10, the client 15 information terminates, unless the client 15 instructs the VVSC to retain a copy of the information in the service request 10.

[0096] The VVSC notifies the individual, the customer 30, whose identity is the subject of said client 15 service request 10. The customer 30 is informed of the time and date the service request 10 is to be fulfilled, that is, the time and date of

the videoconference 40. The customer is instructed what I.D. criteria input 45 is necessary to create 70 and issue 75 the authoritative document 70.

[0097] Upon notification of the service request 10, the customer requiring an identity-based document 70 goes to an independent VVSC 35, that is conveniently located in proximity with their physical location. A videoconference 40 is established between the VVSC and the client 40. The videoconference 40 comprises an infrastructure at each location whereby the customer can input the requested I.D. criteria 45 using a computer networked with the videoconference 40. The customer ID criteria input 45, are at least one of the group of a hard-copy identity document 46, a retina scan 47, a voice print 48, a password/ code 49, a signature 50, a fingerprint 51, or a photograph 52. As the customer I.D. criteria input 45 occurs, the I.D. criteria input 45 is displayed on the screen or the monitor of the requesting governmental agency 15 to the videoconference 40. The I.D. criteria input 45 may be affixed to the authoritative document 70 as a visual representation. Alternatively, the I.D. criteria input 45 may be affixed to the authoritative document 70 in the form of encrypted source code.

[0098] The VVSC verifies 55 the ID criteria input 45 with the client service request 10. If the ID criteria input 45 and the client service request 10 are a match 60, the ID card is created 70, and the ID card is issued 75 to the party

designated in the client 15 service request 10. If the ID criteria input 45 and the client service request 10 do not match 60, the process is terminated 65 until such time the customer can comply with the client service request 10.

[0099] Figure 1 further discloses method of identity verification, whereby the authoritative document 70 is in the form of an identity card 70 for the private sector 15. A private 15 service request 10 is processed in the same manner as a public 15 government agency service request 10. As such, private 15 sector use has been disclosed above. By way of example, private 15 sector use of the present invention is put into context. The client 15 is a university that tenders a service request 10 for an authenticated student identification card 70. The student (customer) need not travel to the university for the creation of the identification card 70 but may go to a VVSC where an authoritative document 70 will be created 70 and issued 75 to the designated party.

[0100] Figures 2- 2C Request for Services from VVSC (Signature Verification)

[0101] In another embodiment of the present invention, the client 15 service request 10 is for signature verification 10 of a customer. In this embodiment, the client 15 may be either a governmental agency or a private party, such as an individual or a bank. With respect to figures 2-2A the two entity types are collectively referred to as the client 15 as depicted in figures 2-2A.

[0102] In the preferred embodiment, a client 15 service request 10 for signature verification discloses a method whereby the signature 50 is notarized 105-115 by a notary public 101. Notarization 105-115 via a videoconference 40 is particularly useful for transactions that require a notary public's 101 signature 50 as a matter of law, such as the transfer of real property. Likewise, notarization 105-115 via a videoconference 40 is particularly useful for transactions that require a notary public's 101 signature 50 for sensitive, legal documents that require notarization 105-115, such as a will or trust.

[0103] In the preferred embodiment, a client 15 tenders a service request 10 for signature verification using a notary public 101 to the VVSC. The service request 10 entails the client 15 selecting the ID criteria 20 to be used to create the authoritative document 70. The service request 10 further includes information necessary for the VVSC to accept the service request 10 (total services requested, client's 15 contact information, customer's contact information). The service request 10 also contains information regarding to whom the authoritative document 70 is to be issued to: either the client, the customer, or a third party designated by the client 15. In the preferred embodiment, the service request 10 specifies that the authoritative document 70 be issued a notarized, enforceable legal document 70.

[0104] Upon receipt of the service request 10, the VVSC accepts the client 15 service request 25. Acceptance entails a VVSC employee registering the service request 10 in a database to manage the service request 10 during the videoconference 40. Registration of information in the service request 10 is for the sole purpose of enabling the request for services 10. Upon completion of the service request 10, the client 15 information terminates, unless the client 15 instructs the VVSC to retain a copy of the information in the service request 10.

[0105] The VVSC notifies the individual, the customer 30, whose signature is the subject of said client 15 service request 10. The customer 30 is informed of the time and date the service request 10 is to be fulfilled, that is, the time and date of the videoconference 40. The customer is instructed what I.D. criteria input 45 is necessary to create 70 and issue 75 the authoritative document 70.

[0106] Upon notification of the service request 10, the customer goes to an independent VVSC 35, that is conveniently located in proximity with their physical location. A videoconference 40 is established between the VVSC and the client 40. The videoconference 40 comprises an infrastructure at each location whereby the customer can input the requested I.D. criteria 45 using a computer networked with the videoconference 40. The customer ID criteria input 45, are at least one of the group of a hard-copy identity document 46, a retina scan 47, a

voice print 48, a password/ code 49, a signature 50, a fingerprint 51, or a photograph 52. As the customer I.D. criteria input 45 occurs, the I.D. criteria input 45 is displayed on the screen or the monitor of the requesting party, the client 15 to the videoconference 40. The I.D. criteria input 45 may be affixed to the authoritative document 70 as a visual representation. Alternatively, the I.D. criteria input 45 may be affixed to the authoritative document 70 in the form of encrypted source code.

[0107] The VVSC verifies 55 the ID criteria input 45 with the client service request 10. If the ID criteria input 45 and the client service request 10 are a match 60, the VVSC enables the document download 90 . If the ID criteria input 45 and the client service request 10 do not match 60, the process is terminated 65 until such time the customer can comply with the client service request 10.

[0108] With reference to Figures 2-2A, document download 90 is from a electronic document repository maintained by the VVSC. The document(s) selected for download 90 are identified in the client 15 service request 10. With respect to Figures 2B-2C, the VVSC uploads 91 a document supplied by the client 15. Either method entails the same process to obtain the customer's signature 50 on the document, and to notarize the document 105-115, if required.

[0109] Each VVSC has access to a host computer where the electronic document has been downloaded 90 or uploaded 91. The electronic document is displayed on a screen or monitor for the respective parties to see, each party viewing the same electronic document during the videoconference 40.

[0110] The customer signs 95 the electronic document by inputting 95 an electronic signature 50 that is affixed to the electronic document. In the preferred embodiment, the customer affixes 95 a graphical, hand-written signature 50 using a signature capture device. In another embodiment, the customer affixes 95 an electronic signature 50 in the form of a digital certificate or source code 49.

[0111] If necessary, the client 15 signs 95 the electronic document by inputting 95 an electronic signature 50 that is affixed to the electronic document. In the preferred embodiment, the client affixes 95 a graphical, hand-written signature 50 using a signature capture device. In another embodiment, the client affixes 95 an electronic signature 50 in the form of a digital certificate or source code 49.

[0112] Upon affixation 95 of each electronic signature 50 to the single electronic document, the VVSC determines whether notarization is required 100. If no, the authoritative document is created 70, the authoritative document is issued 75 to the designated party, and the process terminates 65.

[0113] The notary public 101 may be an employee who is physically located at the VVSC or may be a remote party enjoined by the videoconference 40 by the VVSC. If notarization is required 100, the notary public 101, signs 105 the electronic document by inputting 105 an electronic signature 50 that is affixed to the electronic document. In the preferred embodiment, the notary public 101 affixes 105 a graphical, hand-written signature 50 using a signature capture device. In another embodiment, the notary public 101 affixes 105 an electronic signature 50 in the form of a digital certificate or source code 49.

[0114] After the notary public 101 signs 105 the electronic document, the notary public 101 affixes a notary seal 110 to the electronic document. In the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the electronic notary seal may be affixed to the document in the form of a source code. Upon affixing a notary seal 110 to the electronic document, a notary journal 115 is created and is archived 120.

[0115] The signed, notarized document culminates in the creation of the authoritative document 70, whereby the authoritative document is created 70, and the authoritative document is issued 75 to the party designated in the client

15 service request 10.

[0116] Figs 3-3E Request for Verification Services Via the VVSC Website

[0117] In another embodiment of the present invention, a client accesses the present invention by way of the Internet. In this embodiment, the client tenders a service request from a remote location of theclient's choice, such as the home or the office. In this embodiment of the present invention, the parties to the transaction initiate a videoconference via a website that is a function of the VVSC. The web-based VVSC application has a two-fold function: it allows parties to conduct private transactions using a videoconference broadcast via the WWW (webconference), secondly, and it allows registered users to submit electronic data to the VVSC for retrieval and/or dissemination to other parties.

[0118] With respect to Fig 3D, to use the present invention from a location independent from a VVSC, the private client 15 first must register 195 with the VVSC at the VVSC physical location. The client 15 submits a request registration 195. The registration request 195 requires that the client submit criteria I.D. input 45 to the VVSC. The client I.D. criteria input 45 must contain at least one of the group of a hard-copy identity document 46, a retina scan 47, a voice print 48, a password/ code 49, a signature 50, a fingerprint 51, or a photograph 52.

[0119] With respect to Fig 3E, to use the present invention from a location independent from a VVSC, a public client 15 first must register 195 with the VVSC at the VVSC physical location. The client 15 submits a request registration 195. The registration request 195 requires that the client submit criteria I.D. input 45 to the VVSC. The client I.D. criteria input 45 must contain at least one of the group of a hard-copy identity document 46, a password/ code 49, a signature 50, proof of executive identity/authority, a corporation number 232, or a photograph 52.

[0120] With respect to figs 3-3E, any party desirous of utilizing the VVSC website to enable a service request 10, must have a registration account 210 with the VVSC.

[0121] With respect to Figs 3D-3E, establishing the client 15 registration account 210 comprises the VVSC obtaining the client criteria I.D. input 45 and verifying 205 the client criteria I.D. input 45 from the customer 15 and adding 170 the client criteria I.D input 45 to the registration account 210. Upon registration 210, the VVSC assigns 215 an access code to the registration account 210. The VVSC issues 220 the access code to the client 15. The access code allows the client access to the VVSC website and to utilize the services therein. The VVSC archives 225 the registration account 210.

[0122] The archived registration account 210 contains the client criteria I.D. input 45. The information contained in the archived registration account 210 is used to verify and authenticate a service request tendered through the VVSC website.

[0123] With respect to fig 3A, a client 15 accesses the VVSC 130 website located on the World Wide Web (WWW) by way of a local computer system. The client 15 provides the access code 215 via the local computer system 135. The VVSC determines whether the access code 215 matches 60 the access code 215 archived 225 with the VVSC. If not 61, the client 15 is denied access to the website 61. If yes, the client 15 is granted access to the website 62.

[0124] The client 15 tenders a service request 10 for identity verification via the local computer system 140. The VVSC accepts the client 15 request for services 145. The VVSC notifies the customer of the client request 150. Notification includes providing information on the type service request 10 tendered by the client 15, and the time and date of the videoconference 40 requested by the client.

[0125] The customer accesses the VVSC website via the local computer system 155 and provides the access code 215 via the local computer system 160. The VVSC determines whether the access code 215 matches 60 the access code

215 archived 225 with the VVSC. If not 61, the customer 15 is denied access to the website 61. If yes, the customer 15 is granted access to the website 62.

[0126] A videoconference 40 is established between the VVSC and the client 15 and the customer 15 . The videoconference 40 comprises an infrastructure whereby the client 15 and the customer 15 can input the requested I.D. criteria 45 using a local computer system 165. The customer ID criteria input 45, are at least one of the group of a hard-copy identity document 46, a retina scan 47, a voice print 48, a password/ code 49, a signature 50, a fingerprint 51, or a photograph 52. As the customer I.D. criteria input 45 occurs, the I.D. criteria input 45 is displayed on the screen or the monitor of the local computer system. The I.D. criteria input 45 may be affixed to the authoritative document 70 as a visual representation. Alternatively, the I.D. criteria input 45 may be affixed to the authoritative document 70 in the form of encrypted source code.

[0127] The VVSC verifies the ID criteria input 45 with the client service request 10 by comparing the client I.D. criteria input 45 with the information in the client registration account 210. If the ID criteria input 45 matches the information contained in the client 15 registration account 210, the authoritative document 70 is created 70, and authoritative document is issued 75 to the party designated in the client 15 service request 10. If the ID criteria input 45 and the information

contained in the client 15 registration account 210 do not match 60, the process is terminated 65 until such time the customer can comply with the client service request 10.

[0128] With respect to fig 3B-3C, a client 15 accesses the VVSC 130 website located on the World Wide Web (WWW) by way of a local computer system. The client 15 provides the access code 215 via the local computer system 135. The VVSC determines whether the access code 215 matches 60 the access code 215 archived 225 with the VVSC. If not 61, the client 15 is denied access to the website 61. If yes, the client 15 is granted access to the website 62.

[0129] The client 15 tenders a service request 10 via the local computer system 140 for signature verification using a notary public 101. The VVSC accepts the client 15 request for services 145. The VVSC notifies the customer of the client request 150. Notification includes providing information on the type service request 10 tendered by the client 15, and the time and date of the videoconference 40 requested by the client.

[0130] The customer accesses the VVSC website via the local computer system 155 and provides the access code 215 via the local computer system 160. The VVSC determines whether the access code 215 matches 60 the access code

215 archived 225 with the VVSC. If not 61, the client 15 is denied access to the website 61. If yes, the client 15 is granted access to the website 62.

[0131] A videoconference 40 is established between the VVSC and the client 15 and the customer 15 and the notary public 101. In one embodiment (fig 3A) the client 15 downloads 92 a document from the VVSC electronic repository for signature 50 verification and notarization 105-115. In another embodiment (fig 3B) the client 15 uploads 93 a document from the local computer system for signature 50 verification and notarization 105-115.

[0132] The videoconference 40 comprises an infrastructure whereby the client 15 and the customer 15 can input the requested I.D. criteria 45 using a local computer system 165. The customer ID criteria input 45, are at least one of the group of a hard-copy identity document 46, a retina scan 47, a voice print 48, a password/ code 49, a signature 50, a fingerprint 51, or a photograph 52. As the customer I.D. criteria input 45 occurs, the I.D. criteria input 45 is displayed on the screen or the monitor of the local computer system. The I.D. criteria input 45 may be affixed to the authoritative document 70 as a visual representation. Alternatively, the I.D. criteria input 45 may be affixed to the authoritative document 70 in the form of encrypted source code.

[0133] The VVSC verifies the ID criteria input 45 with the client service request 10 by comparing the client I.D. criteria input 45 with the information in the client registration account 210. If the ID criteria input 45 and the information contained in the client 15 registration account 210 do not match 60, the process is terminated 65 until such time the customer can comply with the client service request 10.

[0134] If the ID criteria input 45 matches 60 the information contained in the client 15 registration account 210, the service request 10 for notarization 105-115 is made possible. The notary public 101, signs 105 the electronic document by inputting 105 an electronic signature 50 that is affixed to the electronic document. In the preferred embodiment, the notary public 101 affixes 105 a graphical, hand-written signature 50 using a signature capture device. In another embodiment, the notary public 101 affixes 105 an electronic signature 50 in the form of a digital certificate or source code 49.

[0135] After the notary public 101 signs 105 the electronic document, the notary public 101 affixes a notary seal 110 to the electronic document. In the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the electronic notary seal may be

affixed to the document in the form of a source code. Upon affixing a notary seal 110 to the electronic document, a notary journal 115 is created and is archived 120.

[0136] The signed, notarized document culminates in the creation of the authoritative document 70, whereby the authoritative document is created 70, and the authoritative document is issued 75 to the party designated in the client 15 service request 10.

[0137] Therefore, the foregoing is considered as illustrative only of the principles of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation shown and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.